DEPOSIT AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Richard BROWN et al.**	Examiner:	Thanhnga B TRUONG
Serial No.:	**10/080,477**	Art Unit:	2135
Filed:	February 22, 2002	Our Ref:	B-4518 619564-1 30006602-2 US
For:	"TRUSTED COMPUTING ENVIRONMENT"	Date:	June 8, 2006
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated January 9, 2006, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed because the Notice of Appeal was filed on April 9, 2006. Please deduct the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 - 18 are the subject of this Appeal and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to establishing and maintaining a trusted computing environment (p. 1 l. 8). More specifically, a trusted computing network or environment can be established or maintained without a computing device being required to directly challenge the trustworthiness of another device when it is required to communicate with that device (p. 6 ll. 8-10).

Claim 1 in particular is directed to a method of operating a trusted computing system comprising a plurality of computing devices on a network, the method comprising an assessor computing device receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 5 ll. 19-22 and ll. 27-29), and the assessor computing device updating via the network the trust policy of a second computing device in accordance with the report (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 9 is directed to a method of operating a trusted computing system comprising a plurality of computing devices on a network, in which a first computing device has a trusted component (p. 4 ll. 5-6) which issues a report pertaining to the trustworthiness of the first computing device (p. 4 ll. 19-21) wherein a trust policy controller receives said report via the network from the trusted component and updates via the network the trust policy of a second computing device in accordance with said report (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 10 is directed to a method of operating a trusted computing system comprising multiple computing devices on a network wherein a trust policy controller determines the trust policy for each of said computing devices (p. 4 ll. 6-17) in accordance with the trustworthiness of other of said multiple computing devices as determined from reports received by the controller

via the network pertaining to the trustworthiness of each computing device (p. 4 ll. 19-23, p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 10 is directed to an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 3 l. 29 – p. 4 l. 7 and p. 4 ll. 19-21), an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device via the network (p. 5 ll. 19-25).

Claim 16 is directed to a system comprising an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 3 l. 29 – p. 4 l. 7 and p. 4 ll. 19-21); an updater for updating the trust policy of a second computing device in accordance with the report; and a transmitter for transmitting the updated policy to the second computing device (p. 5 ll. 19-25). The system further comprises first and second computing devices, wherein at least the first computing device comprises a reporter for sending via the network a trustworthiness report to the assessor computing device and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter (p. 3 l. 27 – p. 4 l. 3).

Claim 18 is directed to a system comprising multiple computing devices on a network, and a trust policy controller which serves to determine the trust policy of said computing devices (p. 3 l. 27 – p. 4 l. 3). Each of the computing devices has associated with it a trust policy memory to store a trust policy for that computing device, and a trusted component which issues a report pertaining to the trustworthiness of that computing device (p. 4 ll. 5-23, p. 5 ll. 1-7), wherein the controller receives via the network reports from the trust components and updates via the network the trust policy in the trust policy memory of each computing device in accordance with the trustworthiness of other of the multiple computing devices as determined from the reports (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-18 are unpatentable under 35 U.S.C. 103(a) over U.S. Pat. No. 5,841,868 to Helbig in view of U.S. Pat. No. 6,289,462 to McNabb et al.

GROUPING OF CLAIMS

For each ground of rejection which Appellants contest herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

ARGUMENT

Issue 1: Whether claims 1-18 are unpatentable under 35 U.S.C. 103(a) over U.S. Pat. No. 5,841,868 to Helbig in view of U.S. Pat. No. 6,289,462 to McNabb et al.

In section 3 of the final Office Action of January 9, the Examiner rejects claims 1-18 under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,841,868 to Helbig in view of U.S. Pat. No. 6,289,462 to McNabb et al. In particular, the Examiner reiterates his opinion that Helbig teaches "an assessor receiving a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report," but "is silent about receiving the report from the authorized card users." The Examiner further finds that McNabb teaches an audit trail comprised of a set of records that enables tracing events forward from original transactions to related records and reports, and backwards from records and reports to their component source transactions. The Examiner continues that "[f]or example, a user initiating a print request from a database application would initially be permitted access only to that portion of the data base that the user is permitted to view based on their role. Each row of a database table may have an extended attribute reflecting the authorization level or role that is required to view that record... In this manner, the report would determine the role of the user to determine the level of the records that may be retrieved." The Examiner finally opines that it would have been obvious of the skilled person to "combine the teaching of McNabb into Helbig's system in which security against unauthorized access is provided" and would have been motivated to do so "wherein to such a

system having security features for enabling control over access to data retained in such a system."

In their reply of October 13, 2005, Appellants noted at the outset that "[t]o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." MPEP §2142. Appellants went on to explain that the Examiner's proffered motivation for the skilled person to attempt the alleged combinations of Helbig and McNabb was in fact not even comprehensible, and that furthermore, "wherein to such a system having security features for enabling control over access to data retained in such a system" did in no way convey where in either McNabb or Helbig the Examiner finds an express suggestion or motivation for the skilled reader of one reference to go looking at the other. Appellants further noted that if the Examiner was attempting to invoke the knowledge generally available to the skilled person, "enabling control over access to data retained in such a system" was completely baseless as in the very same sentence the Examiner acknowledges that in "Helbig's system ... security against unauthorized access is provided." Why would the skilled person attempting to practice Helbig's system, in which security against unauthorized access is provided, feel the need to consult another reference for enabling control over access to data retained in such a system? Appellants expressly noted that they could discern no suggestion or motivation in Helbig that further security features may be needed in his system, and the Examiner had made no attempt at identifying any in the Action.

"Second, there must be a reasonable expectation of success... The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." MPEP §2142. Appellants noted that the Examiner had also offered not one single detail as to how exactly the skilled person would go about combining the teachings of McNabb into the system of Helbig, and submitted that doing so was in fact not possible. McNabb is directed to compartmentalized computer operating systems, and teaches process auditing within this context. Helbig, on the other hand, is directed to controlling physical access to a computer via a smart card. One has nothing to do with the other. How exactly would even a skilled person apply McNabb's principles of applying control and

access attributes to data objects on a server be applied to the system of Helbig, which simply interposes a smart card reader between a computer and its keyboard to control nothing more than the flow of input from the keyboard to the computer? Helbig teaches a way to prevent the keystrokes of a user from reaching the computer's I/O port unless the user is authorized, and it is most certainly not immediately apparent how a skilled person would modify this system with the provision of control and access attributes to data objects for a software executing on the computer, and Appellants once again respectfully submit that the Examiner's broad remarks fall far short of the burden imposed by the Rules and the MPEP.

"Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP §2142. Despite the Examiner's assertions to the contrary, the simple truth is that Helbig and McNabb simply do not disclose all of the claim limitations. Where, for instance, does Helbig teach an assessor, a first computing entity, and a second computing entity? Helbig teaches a computer (i.e. computing entity), a smart card reader, and a human user interacting with both. Which one of these is the assessor? The second computing entity? Furthermore, there is nothing in Helbig that could be understood to correspond to a report pertaining to the trustworthiness of a computing device. At most, Helbig teaches validating the trustworthiness of a human user – this is not the same as receiving a report from a computing device pertaining to the trustworthiness of that computing device.

The Examiner alleges to answer the above in section 4 of the final Action by spending a page and a half's worth of regurgitating the previous Action in support of the assertion that Helbig clearly teaches a trusted computing system, etc. etc., but does not waste one single word on drawing some connection between all this and Appellants' rather clearly worded challenge that (1) there is no motivation or suggestion to combine the references, (2) there is no expectation of success if attempting to combine the references, and (3) the combination of the references would not anticipate each and every claim limitation.

At the middle of page 8 the Examiner does offer the standard paraphrase of *In re Fine* and *In re Jones* and then pithily quips that "in this case, the combination of teachings between Helbig and McNabb is sufficient." The Examiner then swiftly wraps up her "answer" by

counseling Appellants that, indeed, "if the prior art structure is capable of performing the intended use, then it meets the claimed limitations."

The list of questions that the Examiner's "answer" begets is lengthy. What, for instance, is the combination of teachings between Helbig and McNabb sufficient for? Is it sufficient for motivating the skilled person to combine the two references? Or is it sufficient for suggesting to the skilled person that the two references should be combined? Regardless, what the Examiner is in fact asserting is that the combination is sufficient motivation for the combination. The combination, so to speak, begets the combination. This type of circular logic utterly fails to support the Examiner's conclusion. The Examiner appears to not have grasped a fundamental - indeed, the fundamental - tenet of combining references for the purpose of obviating a claim: the skilled person is assumed to start with **one** reference which must provide, by itself, the motivation or suggestion for the skilled person to consult the other reference. The Examiner is apparently alleging that presented, magically, with the *fait accompli* combination of Helbig and McNabb, the skilled person would be properly motivated to combine Helbig and McNabb. Appellants could not agree more, but **this does not meet the Examiner's burden of proof under MPEP §2142**. Appellants thus reiterate: neither Helbig nor McNabb contains any suggestion or motivation for combining the respective reference with the other reference, and the Examiner has made no showing (nor, indeed, even an allegation) of the knowledge generally available to one of ordinary skill in the art that would provide such suggestion or motivation.

The Examiner does not even attempt to address the other two points of Appellants' previous reply, namely that in addition to motivation to combine, the two references –whether individually or in the asserted combination - further lack any expectation of success as well as a complete disclosure of all claim limitations. Appellants are thus left with nothing to respond to, and can but respectfully ask the Appeals Board to consider their arguments as advanced above.

In view of all of the preceding, Appellants respectfully submit that all pending claims as presented are novel and nonobvious over the art of record and that the Examiner's rejection is not in compliance with the Rules nor supported by the art, and thus request that the rejection of all claims be overturned on appeal and the case be passed to allowance.

CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and allowance of the case is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

June 8, 2006
(Date of Transmission)

Shannon Tinsley
(Name of Person Transmitting)

(Signature)

6/8/06
(Date)

Respectfully submitted,

Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Attachments

Claims

1. (previously presented) A method of operating a trusted computing system comprising a plurality of computing devices on a network, the method comprising:

an assessor computing device receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device; and

the assessor computing device updating via the network the trust policy of a second computing device in accordance with the report.

2. (previously presented) A method according to claim 1, wherein the assessor computing device updates via the network the trust policies of multiple computing devices in accordance with the report.

3. (previously presented) A method according to claim 1, wherein the assessor computing device updates via the network policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

4. (previously presented) A method according to claim 1, wherein the assessor computing device updates via the network

policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

5. (previously presented) A method according to claim 1, wherein the assessor computing device requests via the network the first computing device to make the report.

6. (original) A method according to claim 1, wherein the first computing device is caused to report by being started-up or reset, or by an undesirable event occurring.

7. (original) A method according to claim 1, wherein the first computing device is caused to report periodically.

8. (previously presented) A method according to claim 1 in which the second computing device authenticates the trust policy update issued by the assessor computing device before accepting it.

9. (previously presented) A method of operating a trusted computing system comprising a plurality of computing devices on a network, in which a first computing device has a trusted component which issues a report pertaining to the trustworthiness of the first computing device wherein a trust policy controller receives said report via the network from the

trusted component and updates via the network the trust policy of a second computing device in accordance with said report.

10. (previously presented) A method of operating a trusted computing system comprising multiple computing devices on a network wherein a trust policy controller determines the trust policy for each of said computing devices in accordance with the trustworthiness of other of said multiple computing devices as determined from reports received by the controller via the network pertaining to the trustworthiness of each computing device.

11. (previously presented) An assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device via the network.

12. (previously presented) An assessor computing device according to claim 11, wherein the updater is arranged to update the trust policies of multiple computing devices in accordance with the report and the transmitter is arranged to transmit the updated policies to the multiple computing devices via the

network.

13. (previously presented) An assessor computing device according to claim 11, wherein the updater updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

14. (previously presented) An assessor computing device according to claim 11, wherein the updater updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

15. (previously presented) An assessor computing device according to claim 11 further comprising a requestor, for requesting the report from the first computing device.

16. (previously presented) A system, comprising:

an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising

a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device,

an updater for updating the trust policy of a second computing device in accordance with the report, and

a transmitter for transmitting the updated policy to the second computing device, and

the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending via the network a trustworthiness report to the assessor computing device and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter.

17. (original) A system as claimed in claim 16 in which the reporter comprises a trusted component associated with the first computing device.

18. (previously presented) A system, comprising:

multiple computing devices on a network, and

a trust policy controller which serves to determine the trust policy of said computing devices;

each of said computing devices having associated with it a trust policy memory to store a trust policy for that computing device, and a trusted component which issues a report pertaining to the trustworthiness of that computing device; wherein

the controller receives via the network reports from the trust components and updates via the network the trust policy in

the trust policy memory of each computing device in accordance with the trustworthiness of other of said multiple computing devices as determined from said reports.

There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.